Famisanar EPS

Procedimiento: Incidentes de seguridad de la información y protección de datos personales y sensibles

Famisanar	**Famisanar EPS** **Proceso**: Gestión de Tecnología e Innovación **Subproceso**: Gobierno de Tecnología **Procedimiento**: Incidentes de seguridad de la información y protección de datos personales y sensibles	**Código** 04 **Fecha** 2020-07-13 **Versión** 1.0

Propósito

Detectar, contener, eliminar, analizar, reportar y hacer seguimiento a los incidentes de seguridad de la información identificados y reportados por los colaboradores y terceros de la EPS para dar respuesta oportuna incluyendo la activación de controles adecuados para la prevención y la reducción de impactos y la recuperación de ellos.

Responsable

Oficial de Seguridad de la Información y Habeas Data (Gerencia de Tecnología)

Facilitador

Mishell Natali Cortés Sánchez

Entradas y Salidas

Proveedor	Entrada	Procedimiento	Salida	Cliente
1) Atención de Incidentes y Requerimientos 2) Gestión de Seguridad Informática	1) Solicitud de Incidente de seguridad de la información y protección de datos personales y sensibles 2) Solicitud de Incidente de seguridad de la información y protección de datos personales y sensibles	(H) **Incidentes de seguridad de la información y protección de datos personales y sensibles** ***Responsables: Oficial de Seguridad de la Información y Habeas Data (Gerencia de Tecnología)***	1) Solución de incidente, documentación y cierre del caso	1) Mapa de Procesos de EPS Famisanar
			2) Concepto, solicitud de Incidente de seguridad de la información y protección de datos personales	2) Gestión de Seguridad Informática
			3) Registro de incidentes de seguridad de datos personales	3) Registro Nacional de Bases de Datos (RNBD) de la Superintendencia de Industria y comercio - SIC
			4) Reporte de Riesgos Materializados de Incidentes de seguridad o protección de datos personales	4) Dirección de Riesgos

Actividades del Procedimiento

Tarea	Responsable	Descripción	Documentos y/o registros asociados
1. Validar Incidente	Analista de Seguridad	Verificando que realmente es un incidente de seguridad, de lo contrario devolver el ticket a soporte nivel 1 Diligenciando el formato de reporte de incidente de seguridad de acuerdo a la información del usuario. (P-TSSC-F00 REPORTE INCIDENTES SEGURIDAD). Completando descripción del incidente en el ticket de la siguiente forma: Registrando nota con asunto DESCRIPCION Describiendo que, como y porque ocurrió el incidente, consideraciones especiales, impactos adversos, vulnerabilidad identificada, fecha y hora en la que ocurrió. Información adicional del incidente con personas que puedan estar relacionadas o que hayan conocido de la situación.	
2. Investigar y Diagnosticar	Analista de Seguridad	Investigando para dar solución al incidente Realizando un diagnóstico más especializado de la situación Documentando Diagnóstico y cada acción realizada de la siguiente forma: Registrando nota con asunto VALORACION. Describiendo que se observó y que se realizó (mencionar si se utilizó alguna herramienta). Registrando la ubicación exacta de posibles evidencias del incidente. Describiendo como se recolecto la evidencia inicial y detallar si se tuvo algún tipo de custodia o almacenamiento de la evidencia inicial.	
3. Sensibilizar Colaborador	Analista de Seguridad	Enviando correo por medio del ticket con las observaciones pertinentes acerca del incidente presentado al Colaborador, con copia al jefe inmediato. En caso de reincidencia, enviando correo por medio del ticket con las observaciones pertinentes acerca del incidente presentado al Colaborador, con copia al jefe inmediato y Talento Humano.	
4. Escalar a Auditoría	Analista de Seguridad	Enviando correo por medio del ticket e informando las falencias en el proceso detectadas a Auditoría Interna.	
5. Cerrar Incidente	Analista de Seguridad	Categorizando el ticket para el incidente de seguridad de acuerdo a la política descrita en este procedimiento. Completando descripción del incidente en el ticket de la siguiente forma: Registrando nota con asunto RESULTADO. Describiendo las Causas y Oportunidades de Mejora. Cerrando el incidente de acuerdo con el proceso de Gestión de Incidentes.	

6. Convocar Comité De Habeas Data	Analista Protección de Datos	Creando Ticket de tipo Problema de subtipo Habeas Data en la Mesa de Servicios y siguiendo el proceso de Gestión de Problemas con el fin de detectar Causa Raíz, Solución Temporal y Solución Definitiva. Generando informe del o los incidentes presentados con relación a Protección de datos. Convocando el comité de Habeas Data para presentar los incidentes relacionados con Protección de Datos. Registrando la siguiente información en el ticket tipo Problema hasta su finalización: CAUSA RAIZ, SOLUCION TEMPORAL y SOLUCION DEFINITIVA registrando notas con el asunto respectivo. Tipo, Fecha de incidente, Causal, Información Comprometida, Tipo de Información, Cantidad de Titulares Afectados de acuerdo con las políticas establecidas en este procedimiento.	
7. Aprobar Incidentes de Seguridad	Comité Habeas Data	Revisando los incidentes de seguridad relacionados con Protección de Datos. Aprobando los incidentes de protección de Datos a reportar en la SIC. Documentando acerca de la aprobación en el ticket relacionado, con el asunto APROBACIÓN.	
8. Reportar Incidentes de Seguridad	Analista Protección de Datos	Ingresando a la página e ingresando los datos de acceso autorizados. Reportando los incidentes de protección de datos presentados. Recibiendo el número de radicado de la novedad por medio del correo Documentando en el ticket de tipo problema correspondiente. 9. Sensibilizar Colaborador Analista Protección de Datos Enviando correo por medio del ticket con las observaciones	
9. Sensibilizar Colaborador	Analista Protección de Datos	Enviando correo por medio del ticket con las observaciones pertinentes acerca del incidente presentado al Colaborador, con copia al jefe inmediato. En caso de reincidencia, enviando correo por medio del ticket con las observaciones pertinentes acerca del incidente presentado al Colaborador, con copia al jefe inmediato y Talento Humano.	
10. Escalar a Auditoría	Analista Protección de Datos	Enviando correo por medio del ticket e informando las falencias en el proceso detectadas a Auditoría Interna.	
11. Cerrar Incidente	Analista Protección de Datos	Categorizando el ticket para el incidente de seguridad de acuerdo a la política descrita en este procedimiento. Completando descripción del incidente en el ticket de la siguiente forma: Registrando nota con asunto RESULTADO Describiendo las Causas y Oportunidades de Mejora. Cerrando el incidente de acuerdo con el proceso de Gestión de Incidentes.